

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

**REDACTED AFFIDAVIT IN
SUPPORT OF APPLICATION FOR
SEARCH WARRANT**

STATE OF SOUTH DAKOTA)
 :SS
COUNTY OF MINNEHAHA)

I, Adam C. Topping, being first duly sworn upon oath depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Snapchat accounts that are stored at premises owned, maintained, controlled, or operated by Snap Inc. ("Snapchat"), an electronic communications service and/or remote computing service provider headquartered at 2772 Donald Douglas Loop, North Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Snapchat to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) assigned to the Sioux Falls, South Dakota, office. I have worked as a Special Agent with the FBI since March 2, 2008. As part of my duties with the FBI, I investigate violations of federal law, including online exploitation of children, including violations pertaining to the illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have also conducted a wide variety of investigations to include international and domestic terrorism, violent crimes, white collar crimes, and crimes in Indian country. I have gained experience in the conduct of such investigations through previous case investigations, formal training, and in consultation with law enforcement partners in local, tribal, state, and federal law enforcement agencies. I have participated in the execution of numerous warrants to search and seize electronic devices, such as cellular telephones and computers, as well as social media accounts. The following information is based on investigation conducted jointly by the FBI, and local and state law enforcement agencies. This affidavit does not contain the entirety of my knowledge regarding this investigation.

3. I have received information from other law enforcement officers and sources of information by either verbal or written report. The officers and sources providing information may have received the information by way of personal knowledge or from another source.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that [REDACTED], date of birth [REDACTED], 1975, and [REDACTED], date of birth [REDACTED], 1982, were involved in the sex trafficking of [REDACTED], date of birth [REDACTED], 2004, a juvenile, in violation 18 U.S.C. §§ 1591(a)(1) and 1591(a)(2), and possessed child pornography in violation of 18 U.S.C. §§ 2252 and 2252A. There is also probable cause to believe that [REDACTED], date of birth [REDACTED], 1984, the [REDACTED] [REDACTED], was also involved in the sex trafficking of [REDACTED] and financially benefited from the activity in violation of 18 U.S.C. §§ 1591(a)(1) and 1591(a)(2). There is probable cause to search the information described in Attachment A used by [REDACTED] for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE - GENERAL

7. On [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

8. The investigation conducted by me and Detective Jonathan Carda of the Sioux Falls Police Department indicates that [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

PROBABLE CAUSE - ROBERT

9. On [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

10. On [REDACTED]

[REDACTED]

[REDACTED]

11. On [REDACTED]

[REDACTED]

12. On [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13. Subsequent investigation using online resources confirmed that

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

14. On [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

15. On [REDACTED]

[REDACTED]

PROBABLE CAUSE - RONALD AND MELANIE

16. On

[illegible]

17.

17. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

18. On [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

19. Through the use of subpoenas, the FBI obtained records for several

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

20. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

21. Through the use of subpoenas, the FBI obtained [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

22. On [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

23. An examination of [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

PROBABLE CAUSE - SNAPCHAT

24. Based on investigation conducted by myself and Detective Carda, a search warrant issued on [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

25. Obtained via the warrant were Snapchat records for usernames

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

26. Noted in [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

BACKGROUND CONCERNING SNAPCHAT

27. The following language is contained in the Snap Inc. Law Enforcement Guide dated September 29, 2020:

- a. Snapchat is a mobile application made by Snap Inc. ("Snap") and available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats.
- b. Snaps - Snaps are photos or videos taken using the Snapchat app's camera on an individual's mobile device, and may be shared directly with the user's friends, or in a Story (explained below) or Chat. Snap's servers are designed to automatically delete a Snap after it has been opened by all intended recipients. Snap's servers are designed to automatically delete an unopened Snap sent directly to a recipient after 30 days and an unopened Snap in Group Chat after 24 hours.
- c. Stories - A user can add Snaps to their "Story". A Story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to our crowd-sourced service "Our Story", which enables their Snaps to be viewed by all Snapchatters in Search and Snap Map. Snap's servers are designed to automatically delete a Snap in a user's

Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.

- d. Memories - Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called "My Eyes Only"), in which case the content is not accessible to Snap and cannot be decrypted by Snap.
- e. Chat - A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Our servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings. Snap's servers are designed to automatically delete unopened one-to-one chats in 30 days. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not. A user can save a message in Chat by pressing and holding the message. The user can unsave the message by pressing and holding it again. This will delete it from our servers. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat.
- f. Location Data - If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

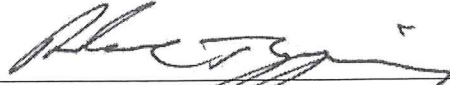
CONCLUSION

28. Based on the foregoing, I request that the Court issue the proposed search warrant.

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Snap Inc. Because the

warrant will be served on Snap Inc., which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Dated this 19th day of May, 2021.



Adam C. Topping, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me, telephonically, on this 19th day of May, 2021.



DANETA L. WOLLMANN
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

REDACTED ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with Snapchat account usernames:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The information sought is stored at premises owned, maintained, controlled, or operated by Snap Inc., a company headquartered at 2772 Donald Douglas Loop, North Santa Monica, California.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

REDACTED ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Snap Inc. ("Snapchat")

To the extent that the information described in Attachment A is within the possession, custody, or control of Snapchat, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Snapchat, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. Subscriber information, including but not limited to, and without date limitation: the names of the accounts; the billing addresses; account registration addresses; passwords; and any email addresses;
- b. Any and all account information, including but not limited to, and without date limitation: user profile including a unique user name, contact information including full names, user identification numbers, birth dates, contact email addresses (including city, state, and zip code), telephone numbers, screen names and other personal identifiers, date of account creation and/or initiations;
- c. Contents of any and all communications or contact, including, but not limited to: read, unread, deleted, drafts of chats; Snaps; Stories and/or time line messages; instant messages; public or private messages and any attachments, including those previously deleted; contents of private mail and/or messages in the user's account

inbox, sent, trash, saved and drafts folders, including those previously deleted; content submitted by this and/or other user to public features. This request is to include any/all EXIF and metadata;

- d. Friends and/or Contact list, and blocked friends list including friends previously deleted from both friends lists and blocked friends list; device phonebook information;
- e. Information regarding filters, queries submitted, time and date of communications, the number of messages exchanged, when a message is opened and a screenshot captured;
- f. Any and all content stored on Snapchat's Memory servers or My Eyes Only pertaining to Snapchat accounts listed in Attachment A including images, video, and photographs, messages, journals, wall posts, comments to status including those previously deleted and/or those removed by Snapchat, including all metadata and EXIF data; images and other information from user device's camera and photos;
- g. Log information including but not limited to: use of services; device information; web browser type and language; access times; pages viewed; identifiers associated with cookies or other technologies that may uniquely identify the user device or browser; and pages visited before or after navigating to the Snapchat website;
- h. IP information, including: addresses at account sign-up; IP history log including the date stamps for the account access, Internet Information Services (IIS) logs, put-get logs, or any other record showing exercise of control or domain over the content or cloud or online digital storage;
- i. Any and all device(s) information for the accounts listed in Attachment A accessing the Snapchat services including without limitation: hardware model, mobile phone number, attributes of the operating system, advertising identifier, unique application identifiers, device settings, browser type, browser information, file and software names and types, battery and signal strength, unique device identifiers (including international mobile equipment identity (IMEI #); mobile equipment identifier (MEID #); electronic serial number (ESN #); mobile station ID (MSID #); international mobile subscriber identity (IMSI #)); mobile operator or Internet Service Provider, language and time zone; device information accessing the Snapchat Service including MAC address and Global Unique Identification (GUID) Number;

- j. Location information including without limitation location information obtained by Snapchat related to any and all devices for the above accounts accessing Snapchat services. This is to include check-ins, precise geographic location using methods that include Global Positioning System (GPS), Bluetooth, wireless networks, Wi-Fi signals GPS, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses; please provide Lat Long records in CSV format.

Facebook is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1591(a)(1), 1591(a)(2), 2252, and 2252A, those violations involving [REDACTED], and/or [REDACTED], and/or [REDACTED], and/or [REDACTED], and occurring from [REDACTED], including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Sex trafficking of a child, possession of child pornography;
- b. Evidence indicating the transfer of funds to/from the account owners which appears related to sex trafficking of a child or child pornography;
- c. Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owners;
- d. Evidence indicating the account owners' states of mind as it relates to the crime under investigation;
- e. The identities of the persons who created or used the usernames, including records that help reveal the whereabouts of such persons; and

- f. The identities of the persons who communicated with the usernames about matters relating to sex trafficking of a child and child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

**REDACTED APPLICATION FOR
SEARCH AND SEIZURE WARRANT**


I, Adam Topping, being first duly sworn, hereby depose and state as follows:

I am a Special Agent with the Federal Bureau of Investigation (FBI) in Sioux Falls, South Dakota, and have reason to believe that within the property fully described in Attachment A, attached hereto and incorporated herein by reference, there is now concealed certain information, namely: that fully described in Attachment B, attached hereto and incorporated herein by reference, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of Title 18 U.S.C. §§ 1591(a)(1) and 1591(a)(2) (sex trafficking of a child), and 18 U.S.C. §§ 2252 and 2252A (sexual exploitation of minors).

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.


Adam C. Topping, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me, telephonically, on the 19th day of May, 2021, at Sioux Falls, South Dakota.


DANETA L. WOLLMANN
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

**REDACTED SEARCH
AND SEIZURE WARRANT**

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement officer or an attorney for the government requests the search of the person and property described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the property described above for the information fully described in Attachment B, attached hereto and incorporated herein by reference, and that such search will reveal evidence of the violations of 18 U.S.C. §§ 1591(a)(1) and 1591(a)(2) (sex trafficking of a child), and 18 U.S.C. §§ 2252 and 2252A (sexual exploitation of minors).

YOU ARE COMMANDED to execute this warrant on or before

June 2, 2021 (not to exceed 14 days)

☐ in the daytime - 6:00 a.m. to 10:00 p.m.

☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the undersigned Judge.

5-19-21 at 2:00^{PM} MT at Sioux Falls, South Dakota
Date and Time Issued Telephonically



DANETA L. WOLLMANN
United States Magistrate Judge

cc: AUSA Clapper - clr

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

REDACTED RETURN

Date and time warrant executed: _____

Copy of warrant and inventory left with: _____

Inventory made in the presence of: _____

Inventory of the property taken and name of any person(s) seized (attach additional sheets, if necessary):

CERTIFICATION
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.
Adam C. Topping, Special Agent Federal Bureau of Investigation

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

REDACTED ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with Snapchat account
usernames:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The information sought is stored at premises owned, maintained,
controlled, or operated by Snap Inc., a company headquartered at 2772 Donald
Douglas Loop, North Santa Monica, California.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 4:21-mj-79

21-083-04

REDACTED ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Snap Inc. ("Snapchat")

To the extent that the information described in Attachment A is within the possession, custody, or control of Snapchat, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Snapchat, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. Subscriber information, including but not limited to, and without date limitation: the names of the accounts; the billing addresses; account registration addresses; passwords; and any email addresses;
- b. Any and all account information, including but not limited to, and without date limitation: user profile including a unique user name, contact information including full names, user identification numbers, birth dates, contact email addresses (including city, state, and zip code), telephone numbers, screen names and other personal identifiers, date of account creation and/or initiations;
- c. Contents of any and all communications or contact, including, but not limited to: read, unread, deleted, drafts of chats; Snaps; Stories and/or time line messages; instant messages; public or private messages and any attachments, including those previously deleted; contents of private mail and/or messages in the user's account

inbox, sent, trash, saved and drafts folders, including those previously deleted; content submitted by this and/or other user to public features. This request is to include any/all EXIF and metadata;

- d. Friends and/or Contact list, and blocked friends list including friends previously deleted from both friends lists and blocked friends list; device phonebook information;
- e. Information regarding filters, queries submitted, time and date of communications, the number of messages exchanged, when a message is opened and a screenshot captured;
- f. Any and all content stored on Snapchat's Memory servers or My Eyes Only pertaining to Snapchat accounts listed in Attachment A including images, video, and photographs, messages, journals, wall posts, comments to status including those previously deleted and/or those removed by Snapchat, including all metadata and EXIF data; images and other information from user device's camera and photos;
- g. Log information including but not limited to: use of services; device information; web browser type and language; access times; pages viewed; identifiers associated with cookies or other technologies that may uniquely identify the user device or browser; and pages visited before or after navigating to the Snapchat website;
- h. IP information, including: addresses at account sign-up; IP history log including the date stamps for the account access, Internet Information Services (IIS) logs, put-get logs, or any other record showing exercise of control or domain over the content or cloud or online digital storage;
- i. Any and all device(s) information for the accounts listed in Attachment A accessing the Snapchat services including without limitation: hardware model, mobile phone number, attributes of the operating system, advertising identifier, unique application identifiers, device settings, browser type, browser information, file and software names and types, battery and signal strength, unique device identifiers (including international mobile equipment identity (IMEI #); mobile equipment identifier (MEID #); electronic serial number (ESN #); mobile station ID (MSID #); international mobile subscriber identity (IMSI #)); mobile operator or Internet Service Provider, language and time zone; device information accessing the Snapchat Service including MAC address and Global Unique Identification (GUID) Number;

- j. Location information including without limitation location information obtained by Snapchat related to any and all devices for the above accounts accessing Snapchat services. This is to include check-ins, precise geographic location using methods that include Global Positioning System (GPS), Bluetooth, wireless networks, Wi-Fi signals GPS, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses; please provide Lat Long records in CSV format.

Facebook is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1591(a)(1), 1591(a)(2), 2252, and 2252A, those violations involving [REDACTED], and/or [REDACTED], and/or [REDACTED], and/or [REDACTED], and occurring from [REDACTED], including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Sex trafficking of a child, possession of child pornography;
- b. Evidence indicating the transfer of funds to/from the account owners which appears related to sex trafficking of a child or child pornography;
- c. Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owners;
- d. Evidence indicating the account owners' states of mind as it relates to the crime under investigation;
- e. The identities of the persons who created or used the usernames, including records that help reveal the whereabouts of such persons; and

- f. The identities of the persons who communicated with the usernames about matters relating to sex trafficking of a child and child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.